THE COMMITTEE ON ENERGY AND COMMERCE

INTERNAL MEMORANDUM

May 31, 2011

To: Members of the Subcommittee on Commerce, Manufacturing, and Trade

From: Majority Committee Staff

Re: Hearing on "Sony and Epsilon: Lessons for Data Security Legislation"

I. Summary

On Thursday, June 2, 2011, the Subcommittee on Commerce, Manufacturing, and Trade will hold a hearing entitled, "Sony and Epsilon: Lessons for Data Security Legislation" in 2123 Rayburn House Office Building. The hearing will convene 15 minutes after the conclusion of the Full Committee markup. Witnesses are by invitation only.

The purpose of this hearing is to examine the risks of the recent historic data breaches at Epsilon and Sony and the state of the ongoing investigations into each incident.

II. Witnesses

Two witnesses will testify before the Subcommittee:

Jeanette Fitzgerald, General Counsel, Epsilon Data Management, LLC

Tim Schaaff, President, Sony Network Entertainment International

III. Background

The Subcommittee on Commerce, Manufacturing, and Trade held a hearing on data security on May 4, 2011. The topic of the hearing was the ongoing threat of data breaches to consumers. Within the month preceding that hearing, two high profile breaches occurred: Epsilon and Sony PlayStation Network. Both companies were invited to participate in the hearing but declined on the basis that their internal investigations were ongoing. Additionally, Sony asserted that its efforts to patch the security "hole" were ongoing at that time as well.

Epsilon

Epsilon Data Management is a business-to-business marketing services firm that manages email marketing campaigns for approximately 2500 companies. On April 1, 2011, Epsilon announced a criminal intrusion into their servers. While Epsilon initially estimated 50 of its corporate customers were affected, more recent media reports indicate the breach impacted about 75 of those firms (approximately 3 percent of their customers). Among those affected by the breach are customers of Kroger, JPMorgan Chase, Capitol One, Citibank, Best Buy, Verizon, Target, Home Shopping Network, and Verizon. Hackers acquired access to email addresses and,

in some cases, customer names. Conservative estimates put the number of affected email accounts around 60 million.

Sony

The Epsilon data breach was soon overshadowed by a criminal hack into Sony's PlayStation Network servers. Sony announced on April 22, 2011, that an intrusion had occurred on April 19, affecting 77 million accounts. Intruders gained access to personal information such as name, email address, passwords, physical address, and birthdates.[1] After reportedly patching the security hole and having determined what information was accessed, Sony began notifying the holders of the 77 million accounts on April 26, 2011.[2] Due to the sheer number of accounts affected, Sony did not complete notification until 6 days after the notice began. Sony resumed its PlayStation Network operations to North America and Europe on May 15, and it restored access to Japan on May 27.

On May 2, 2011, Sony announced what appeared to be a related breach of its Sony Online Entertainment network. On May 1, 2011, Sony discovered intruders gained access to nearly 25 million users' information in approximately mid-April. That breach involved access to name, address, email addresses, birthdates, gender, phone number, and login name and password.

On May 21, Sony reported a breach of So-Net Entertainment Corp, an ISP service in Japan. That intruder gained access to 90 of its users' email accounts in addition to compromising the rewards points accounts of approximately 200 accounts.

Last week, Sony announced yet another two breaches. On May 24, Sony announced it discovered a security breach of its music service in Greece, impacting 8,500 accounts. No credit card information was taken, but names, phone numbers, and email addresses may have been breached. On May 25, Sony announced a breach affecting approximately 2,000 Canadian Sony Ericsson Mobile Communications customers. The breach compromised those customers' usernames, passwords, and email addresses. Sony has not yet determined whether each of the incidents is related.

Formal Inquiries

To inform the Committee's efforts in the data security and data breach notification arena, Chairman Bono Mack and Ranking Member Butterfield sent a series of inquiries to both Epsilon and Sony.

- April 6, 2011: Chairman Bono Mack and Ranking Member Butterfield to Epsilon

[1] While the intruders had access to the server containing credit card information, there is no evidence that such information was taken, unlike the rest of the personal information where the intruders left indications of data transfer.
[2] Users and accounts are distinguishable as some users have more than one account.

http://republicans.energycommerce.house.gov/Media/file/Letters/112th/040611alliance.pdf

- April 18, 2011: Epsilon response

http://republicans.energycommerce.house.gov/Media/file/Letters/041811%20Epsilon%20Response.pdf

- April 29, 2011: Chairman Bono Mack and Ranking Member Butterfield to Sony

http://republicans.energycommerce.house.gov/Media/file/Letters/112th/042911sony.pdf

- May 3, 2011: Sony response

http://republicans.energycommerce.house.gov/Media/file/Letters/112th/050411Hirai.pdf

- May 17, 2011: Chairman Bono Mack and Ranking Member Butterfield to Sony

http://republicans.energycommerce.house.gov/Media/file/Letters/112th/051711Sony.pdf

- May 26, 2011: Sony response

http://republicans.energycommerce.house.gov/Media/file/Letters/112th/052611sonyresponse.pdf

IV. Data Security Legislation

While more than 45 States and U.S. territories have each enacted data breach notification requirements, with the exception of notification requirements for breached health information, there is no Federal data breach notification law. As a result of the confusing and often overlapping or contrary patchwork of State notification laws, Rep. Stearns (the then-Chairman of the Subcommittee on Commerce, Trade, and Consumer Protection) introduced H.R. 4127, the Data Accountability and Trust Act (DATA) in the 109th Congress. The bill established national standards for (1) security requirements for entities holding personal information to protect against unauthorized access; (2) notification procedures to affected consumers upon a breach; and (3) special requirements for information brokers. It charged the Federal Trade Commission (FTC) with enforcement. The Committee reported H.R. 4127 on a bipartisan basis, but the bill did not proceed to the full House for a vote as a result of disagreements with other committees regarding jurisdiction that could not be resolved before the Congressional calendar expired.

In the 110th Congress, then-Chairman Rush re-introduced the text of H.R. 4127 as reported by the Committee as H.R. 958 but the legislation received no Committee action. In the 111th Congress, Rep. Rush again reintroduced DATA as H.R. 2221. H.R. 2221 processed through the Committee on a bipartisan basis and passed the House, as amended, by voice vote on December 8, 2009. As reported, H.R. 2221:

- Required entities that hold personal information to establish and maintain appropriate security policies to prevent unauthorized acquisition of that data.

- Required companies to notify consumers in the event of a breach of personally identifiable information that results in a reasonable risk of identity theft or fraud.
- Imposed special requirements on information brokers (those entities that compile and sell consumer data to third parties) including assuring accuracy of their information, allowing consumer access to their records and the ability to correct inaccurate information.
- Superseded State data breach and notification laws but permitted enforcement by State Attorneys General with an aggregate cap on damages.
- Preempted similar State laws to create a uniform national standard for data security and breach notification.
- Mandated reasonable security practices for paper records containing personally identifiable information.
- Permitted an information broker to include intentionally false information in a database if used for fraud detection purposes and the information is identified as inaccurate.
- Allowed for a delay in breach notification for law enforcement or national security purposes.
- Added passport numbers and military ID numbers to the definition of personal information.

Chairman Bono Mack intends to introduce a data security and notification bill after receiving comments through Subcommittee oversight and a relevant stakeholder process.

Please contact Brian McCullough, Gib Mullan, or Shannon Weinberg at ext. 5-2927 with any questions.